

**THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF MISSOURI**

**IN THE MATTER OF THE
SEARCH OF
1140 SOUTH GRANT AVENUE
SPRINGFIELD, MISSOURI 65807**

18-SW-208DPR

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, James D. Holdman Jr., being first duly sworn, do hereby depose and state that:

1. This affiant is a Special Agent (SA) with United States Immigration and Customs Enforcement (ICE) Office of Homeland Security Investigations (HSI) in Springfield, Missouri. This affiant has been employed with ICE/HSI since June 2003. This affiant has been employed in the field of law enforcement since January 1989, including duties as a deputy sheriff in Washington County, Missouri, and a criminal investigator for the State of Missouri.
2. As part of this affiant's duties with ICE/HSI, this affiant investigates criminal violations relating to child exploitation, child pornography, human trafficking, and coercion and enticement, in violation of 18 U.S.C. §§ 2251, 2422(a) and (b), 2252(a), and 2252A. This affiant has received training in the areas of child pornography, child exploitation, and human/sex trafficking,
3. This affiant has conducted operations relating to the exploitation of children and adults in Costa Rica, the United States, and the Philippines. This affiant has instructed classes on sexual exploitation of children, interviewing, evidence collection, case studies, and undercover operations to law enforcement agencies within the United States, including

six national conferences, as well as to law enforcement located in the following foreign countries:

- a. Cambodian National Police in Phnom Penh and Siem Reap;
- b. International Law Enforcement Academy (ILEA) in El Salvador;
- c. Moroccan Police Academy in Kenitra;
- d. Ontario Canada Provincial Police in Niagara Falls, Canada; and
- e. Royal Canadian Mounted Police Headquarters, Ottawa, Canada.

4. The statements in this affidavit are based on personal observations, training and experience, investigation of this matter, and information obtained from other agents and witnesses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, this affiant has not included each and every fact known to me concerning this investigation. This affiant has set forth the facts necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252, and 2252A are currently located at 1140 South Grant Avenue, Springfield, Missouri, which is located in the Western District of Missouri.

5. This affidavit is in support of an application for a search warrant for evidence, fruits, and instrumentalities of the forgoing criminal violations, which relate to the knowing possession, receipt, distribution, and production of child pornography. The property to be searched is described in the following paragraphs and in Attachment A. This affiant requests the authority to search and/or examine the seized items, specified in Attachment B, as instrumentalities, fruits, and evidence of crime.

6. This affiant has probable cause to believe that evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, involving the use of a computer in or affecting interstate commerce to receive, distribute, possess, and produce child pornography, are located in and within the aforementioned property described below. Thus, as outlined below, and based on my training and experience, there is probable cause to believe that evidence, fruits and/or instrumentalities of the aforementioned crimes are located in this property.

STATUTORY AUTHORITY

7. This investigation concerns alleged violations of Title 18, United States Code, §§ 2251, 2252, and 2252A, relating to material involving the sexual exploitation of minors:
- a. 18 U.S.C. § 2251(a) prohibits a person from employing, using, persuading, inducing, enticing or coercing a minor to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce, or if such visual depiction actually was transported in or affecting interstate commerce.
 - b. 18 U.S.C. § 2252 prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or

foreign commerce.

- c. 18 U.S.C. § 2252A prohibits a person from knowingly mailing, transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. §2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

DEFINITIONS

8. The following definitions apply to this Affidavit and its Attachments:

- a. The term “minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.
- b. The term “sexually explicit conduct,” 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.
- c. The term “visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted

by any means, whether or not stored in a permanent format.

- d. The term “computer,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
- e. The term “child pornography,” as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where
 - 1. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
 - 2. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
 - 3. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
- f. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, and painting), photographic form (including, but not limited to, microfilm,

microfiche, prints, slides, negatives, videotapes, motion pictures, and photocopies), mechanical form (including, but not limited to, phonograph records, printing, and typing) or electrical, electronic, or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

- g. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
- h. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.

- i. “Domain names” are common, easy to remember names associated with an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.
- j. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

- 9. Based on this affiant’s knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom this affiant has had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.
- 10. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking.
- 11. With digital cameras, images of child pornography can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.
- 12. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly

referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

13. The Internet affords individuals several different venues for meeting on another, obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.
14. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.
15. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the

computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

CELLULAR PHONES AND CHILD PORNOGRAPHY

16. Based on this affiant’s knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement

officers with whom this affiant has had discussions, cellular phones have likewise revolutionized the manner in which child pornography is produced and distributed.

17. Cellular phones (“cell phones”) are exceptionally widespread. The Central Intelligence Agency estimates that in 2009 there were 286 million cell phone subscribers in the United States. Cell phones increasingly offer features such as integrated digital cameras, the ability to store hundreds of digital images, and the ability to access and browse the Internet.
18. In this affiant’s training and experience, the ready availability and personal nature of cell phones has led to their frequent use in the commission of child pornography offenses. Individuals with a sexual interest in children will often use their cell phone to browse the Internet and to distribute, receive, and store child pornography files. Individuals producing child pornography will also frequently use the integrated digital camera within a cell phone to produce the images, and then store the images both on the phone and on other devices – such as computers and computer storage media.
19. Cell phones, like other computer systems, will frequently retain data relating to activities, such as Internet browsing history, digital images, and other digital data, that can remain stored for a long period of time.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND CELL PHONES

20. Searches and seizures of evidence from computers and cell phones commonly require agents to download or copy information from the devices and their components, or seize most or all computer items (computer hardware, computer software, and computer related

documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish fully on-site.
- b. Searching computer systems and cell phones for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious

code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

21. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (“CPU”). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).
22. Furthermore, because there is probable cause to believe that the computer, its storage devices and cell phones are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

BACKGROUND OF INVESTIGATION

23. On Friday, July 14, 2017, at 09:15 a.m., Southwest Missouri Cyber Crimes Task Force (SMCCTF) Officer James Smith initiated an investigation into a device, using IP address 173.24.243.102, possibly involved in distributing child pornography on the Gnutella2 peer-to-peer network.
24. Peer to Peer (P2P) file sharing, specifically the operation of the Gnutella networks, are P2P networks used to exchange files between computers. The Gnutella networks, like other P2P file sharing networks, use file hashing to uniquely identify files on the network, and users typically locate files with keyword searches.
25. On July 14, 2017, Task Force Officer (TFO) Smith made a direct connection with the

suspect device at IP address 173.24.243.102, the program reported itself as Shareaza 2.7.9.0, and transmitted a user created nickname of "Robert." Between 3:07 p.m. and 3:48 p.m., TFO Smith was able to obtain a portion of a file titled: "BEAUTIFUL_Venezuela-girls(3-4yo)part-2) pthc hussyfan_Pedo FuX Makes A Childs Cute Peepee Orgasm`s Happen-Precious_!! Kids NEED Sex TOO_!!.mpg." Additional portions of the file were successfully downloaded between 4:29 p.m. and 11:15 p.m. The remaining portions of the file were downloaded on July 15, 2017.

26. TFO Smith viewed the downloaded file and described it as follows:

- a. The video depicts two nude prepubescent girls, two to four years of age, in a bathtub rubbing an adult male's penis. As the video continues, another person's legs can be seen setting on the edge of the tub with their feet in the water, holding one of the girls in place. The child masturbating the male appears to be following commands, and opens her mouth for a moment, but then begins shaking her head no. The other child then begins masturbating the male penis and performs oral sex on the male. At approximately 1 minute, 30 seconds, the video cuts to a nude prepubescent child, similar to one of the girls in the tub earlier, lying back on a bed with her legs in the air. The video zooms in on the child's pubic area to reveal her being masturbated utilizing a sex toy. The child is then anally and vaginally penetrated by an adult male's penis, with the male ultimately ejaculating on the child's vagina.

27. A portion of five additional files of note were received from the suspect device between July 15, 2017, and July 20, 2017, titled as follows:

- a. "Real Private Daughter (cd found on Landfill) stolen pedo lolita pthc
hussyfan preteen nude (12-13Y) 05.jpg
CHFZWCQ2P2YYO32T5NVRKRXU7KWLNIWF;"
- b. "9Y Daughter Anal Fuck With Dad Pthc R@Ygold Child Kid Pedo Hentai
Manga Slut Suck Lolita.avi
Z3NCGBCM2RZ5WGSG6KDXHNKPACPYR3JD;"
- c. "TTJF & H [B - 2mn26s - son direct - fillette blonde, fellation] pthc Pedoland
Frifam 2007 New Girl Img 0167.avi
VW3OYWNSXQBYC6UQRBOF7A6FEOOQZZBY;"
- d. "[boy+man] 2 mans n boy (Pthc) Mes1 - Gay - Bj And Anal With Young
Boy - 14m35S.avi SNJGTDQP43BDGMFMEFJA5B4VR4HOMVHJ;" and
- e. "@Pthc - Toddler Nice Orgasm From 4Yo Girl 2011.mpg
YTJKNNKU4XHTWR32J3IP2GRWFTOX7VD3."

28. TFO Smith viewed each of the files and determined that each file contained a depiction of a child or children engaged in some sort of sexual contact with others and/or exposing their genitals to the camera in a lewd and lascivious manner.

29. The computer at IP Address 173.24.243.102 was the sole candidate for these downloads, and as such, the entire files, or portions thereof, were downloaded directly from this IP Address.

30. On Monday, July 17, 2017, TFO Smith conducted a query on the IP address 173.24.243.102 through the American Registry for Internet Numbers (ARIN). ARIN reported that IP address 173.24.243.102 is registered to Mediacom Communications

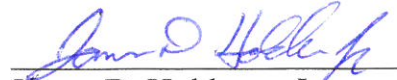
Corporation.

31. On Monday, July 17, 2017, TFO Smith requested an investigative subpoena to be issued to Mediacom Communications Corp. for subscriber information on IP address 173.24.243.102, between July 15, 2017, and July 16, 2017.
32. On Wednesday, July 19, 2017, Mediacom Communications Corporation, in compliance with the subpoena, reported that IP address 173.24.243.102 was assigned to their subscriber Robert Huynh, with a service address of 1140 South Grant Avenue, Springfield, Missouri, 65807, between July 15, 2017, and July 16, 2017.
33. On Wednesday, December 13, 2017, TFO Smith checked the status of IP address 173.24.243.102, and determined that the device was making several files known to contain depictions of child pornography available for download..
34. On December 13, 2017, this affiant conducted surveillance at 1140 South Grant Avenue, Springfield, Missouri, and took a photograph of the residence as shown in Attachment A. This affiant confirmed through a record check with the Missouri Department of Revenue that Robert “Phuoc” Tan Huynh has a current address of 1140 South Grant Avenue in Springfield, Missouri.

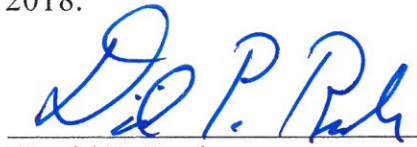
PROBABLE CAUSE

35. Based on the above facts, this affiant believes probable cause exists for the issuance of a warrant to search the premises described more fully in Attachment A for (1) property that constitutes evidence of the commission of a criminal offense; (2) contraband, the fruits of a crime, or things otherwise criminally possessed; and/or (3) property designated or intended for use or which is or has been used as the means of committing a criminal

offense, namely possible violations of Title 18, United States Code, Sections 2251, 2252, and 2252A, including but not limited to the items listed in Attachment B.


James D. Holdman, Jr.
Special Agent
Homeland Security Investigations

Subscribed and sworn before me this 14th day of February, 2018.


David P. Rush
United States Magistrate Judge
Western District of Missouri